

Vertex connectivity of the power graph of a finite cyclic group

Sriparna Chattopadhyay

Kamal Lochan Patra

Binod Kumar Sahoo

Abstract

Let $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, where r, n_1, \dots, n_r are positive integers and p_1, p_2, \dots, p_r are distinct prime numbers with $p_1 < p_2 < \cdots < p_r$. For the cyclic group C_n of order n , let $\mathcal{P}(C_n)$ be the power graph of C_n and $\kappa(\mathcal{P}(C_n))$ be the vertex connectivity of $\mathcal{P}(C_n)$. Clearly, $\kappa(\mathcal{P}(C_n)) = p_1^{n_1} - 1$ if $r = 1$. So assume that $r \geq 2$. We determine $\kappa(\mathcal{P}(C_n))$ when $2\phi(p_1 \cdots p_{r-1}) \geq p_1 \cdots p_{r-1}$. If $2\phi(p_1 \cdots p_{r-1}) < p_1 \cdots p_{r-1}$, then we give an upper bound for $\kappa(\mathcal{P}(C_n))$ which is sharp for many values of n .

Key words: Power graph, Vertex connectivity, Cyclic group, Euler's totient function

AMS subject classification. 05C25, 05C40

1 Introduction

The concept of directed power graph of a group was introduced by Kelarev et al. in [9], which was further extended to semigroups in [10, 11]. Chakrabarty et al. defined the notion of undirected power graph of a semigroup, in particular, of a group in [3]. Since then many researchers have investigated both directed and undirected power graphs of semigroups from different view points. For more on these graphs, we refer the reader to the survey paper [1] and the references therein. One can refer to [8] and [13] for some recent related works in this direction.

The *power graph* $\mathcal{P}(G)$ of a group G is the simple undirected graph with vertex set G , in which two distinct vertices are adjacent if and only if one of them can be obtained as an integral power of the other. If G is a finite group, then the identity element is adjacent to all other vertices and so $\mathcal{P}(G)$ is connected. Here we consider $G = C_n$, a finite cyclic group of order n , where n is a positive integer. The graph $\mathcal{P}(C_n)$ has maximum number of edges among all the power graphs of finite groups of order n . This property of $\mathcal{P}(C_n)$ was conjectured by Mirzargar et al. in [12] and proved by Curtin and Pourgholi in [6]. The clique number, the chromatic number and the independence number of $\mathcal{P}(C_n)$ were determined/described in [12]. In this paper, we study the vertex connectivity of $\mathcal{P}(C_n)$ which is denoted by $\kappa(\mathcal{P}(C_n))$.

Recall that $\kappa(\mathcal{P}(C_n))$ is the minimum number of vertices which need to be removed from the vertex set C_n so that the induced subgraph of $\mathcal{P}(C_n)$ on the remaining vertices is disconnected or has only one vertex. If $n = 1$, then clearly $\kappa(\mathcal{P}(C_1)) = 0$. If n is divisible by only one prime number, that is, if $n = p^m$ for some prime p and some positive integer m , then $\mathcal{P}(C_{p^m})$ is a complete graph (see [3, Theorem 2.12] for the converse statement) and so $\kappa(\mathcal{P}(C_{p^m})) = p^m - 1$.

For the rest of the paper, we assume that n is divisible by at least two distinct prime numbers. We write the prime power decomposition of n as

$$n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$

where $r \geq 2$, n_1, \dots, n_r are positive integers and p_1, \dots, p_r are distinct prime numbers with

$$p_1 < p_2 < \cdots < p_r.$$

Since $r \geq 2$, the identity element and the generators of C_n are precisely the vertices of $\mathcal{P}(C_n)$ which are adjacent to all other vertices (see [2, Proposition 4] for the general statement). Therefore, in order to find $\kappa(\mathcal{P}(C_n))$, the first step should be to remove these vertices and this gives

$$\kappa(\mathcal{P}(C_n)) \geq \phi(n) + 1, \quad (1)$$

where $\phi : \mathbb{N} \rightarrow \mathbb{N}$ is the Euler's totient function. Note that the number of generators of C_n is $\phi(n)$. If $n = p_1 p_2$, then equality holds in (1) by [4, Theorem 3(ii)]. We shall show that the converse is also true (see Lemma 2.5). When $n = p_1^{n_1} p_2^{n_2}$, it was proved in [5, Theorem 2.7] that

$$\kappa(\mathcal{P}(C_n)) \leq \phi(n) + p_1^{n_1-1} p_2^{n_2-1}.$$

If $n = p_1 p_2 p_3$, then [5, Theorem 2.9] gives that

$$\kappa(\mathcal{P}(C_n)) \leq \phi(n) + p_1 p_2 - \phi(p_1 p_2).$$

1.1 Main Results

For a given subset X of C_n , we define $\overline{X} = C_n \setminus X$ and denote by $\mathcal{P}(\overline{X})$ the induced subgraph of $\mathcal{P}(C_n)$ with vertex set \overline{X} . In this paper, we prove the following in Sections 3 and 4.

Theorem 1.1. *Let $n = p_1^{n_1} \cdots p_r^{n_r}$, where $r \geq 2$, n_1, \dots, n_r are positive integers and p_1, \dots, p_r are distinct prime numbers with $p_1 < p_2 < \cdots < p_r$. Then the following hold:*

(i) *If $2\phi(p_1 \cdots p_{r-1}) > p_1 \cdots p_{r-1}$, then*

$$\kappa(\mathcal{P}(C_n)) = \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})].$$

Further, there is only one subset X of C_n with $|X| = \kappa(\mathcal{P}(C_n))$ such that $\mathcal{P}(\overline{X})$ is disconnected.

(ii) *If $2\phi(p_1 \cdots p_{r-1}) < p_1 \cdots p_{r-1}$, then*

$$\kappa(\mathcal{P}(C_n)) \leq \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} [p_1 \cdots p_{r-1} + \phi(p_1 \cdots p_{r-1})(p_r^{n_r-1} - 2)].$$

(iii) *If $2\phi(p_1 \cdots p_{r-1}) = p_1 \cdots p_{r-1}$, then $r = 2$, $p_1 = 2$ (so that $n = 2^{n_1} p_2^{n_2}$) and*

$$\kappa(\mathcal{P}(C_n)) = \phi(n) + 2^{n_1-1} p_2^{n_2-1}.$$

Moreover, there are n_2 number of subsets X of C_n with $|X| = \kappa(\mathcal{P}(C_n))$ for which $\mathcal{P}(\overline{X})$ is disconnected.

As a consequence of Theorem 1.1(i) and (iii), we obtain the following when the smallest prime divisor of n is at least the number of distinct prime divisors of n .

Corollary 1.2. *If $p_1 \geq r$, then*

$$\kappa(\mathcal{P}(C_n)) = \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})].$$

In order to show that the bound in Theorem 1.1(ii) is sharp for certain values of n , we prove the following in Section 5 when $r = 3$.

Theorem 1.3. *Let $n = p_1^{n_1} p_2^{n_2} p_3^{n_3}$, where n_1, n_2, n_3 are positive integers and p_1, p_2, p_3 are distinct prime numbers with $p_1 < p_2 < p_3$. If $2\phi(p_1 p_2) < p_1 p_2$, then $p_1 = 2$ and*

$$\kappa(\mathcal{P}(C_n)) = \phi(n) + 2^{n_1-1} p_2^{n_2-1} [(p_2 - 1) p_3^{n_3-1} + 2].$$

Further, there is only one subset X of C_n with $|X| = \kappa(\mathcal{P}(C_n))$ such that $\mathcal{P}(\overline{X})$ is disconnected.

The situation left is when $r \geq 4$ and $2\phi(p_1 \cdots p_{r-1}) < p_1 \cdots p_{r-1}$, for which we conjecture that equality should hold in Theorem 1.1(ii). Note that the values in Theorem 1.1 are equal if $n_r = 1$.

2 Preliminaries

Recall that ϕ is a multiplicative function, that is, $\phi(ab) = \phi(a)\phi(b)$ for any two positive integers a, b which are relatively prime. So

$$\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdots p_r^{n_r-1}(p_r - 1) = p_1^{n_1-1} \cdots p_r^{n_r-1} \phi(p_1 p_2 \cdots p_r).$$

Lemma 2.1. *For $1 \leq i \leq r - 1$, we have*

$$\phi\left(\frac{n}{p_i}\right) \geq \phi\left(\frac{n}{p_r^{n_r}}\right) p_r^{n_r-1},$$

where the inequality is strict except when $r = 2$, $p_1 = 2$, $p_2 = 3$ and $n_1 \geq 2$.

Proof. Let $1 \leq i \leq r - 1$. We have $\phi(p_r) = p_r - 1 \geq p_i > p_i - 1 = \phi(p_i)$. If $n_i = 1$, then

$$\begin{aligned} \phi\left(\frac{n}{p_i}\right) &= p_1^{n_1-1} \cdots p_{i-1}^{n_{i-1}-1} p_{i+1}^{n_{i+1}-1} \cdots p_r^{n_r-1} \phi(p_1 \cdots p_{i-1} p_{i+1} \cdots p_r) \\ &> p_1^{n_1-1} \cdots p_{i-1}^{n_{i-1}-1} p_{i+1}^{n_{i+1}-1} \cdots p_r^{n_r-1} \phi(p_1 \cdots p_i \cdots p_{r-1}) = \phi\left(\frac{n}{p_r^{n_r}}\right) p_r^{n_r-1}. \end{aligned}$$

If $n_i \geq 2$, then

$$\begin{aligned} \phi\left(\frac{n}{p_i}\right) &= p_1^{n_1-1} \cdots p_{i-1}^{n_{i-1}-1} p_i^{n_i-2} p_{i+1}^{n_{i+1}-1} \cdots p_r^{n_r-1} \phi(p_1 p_2 \cdots p_r) \\ &\geq p_1^{n_1-1} \cdots p_i^{n_i-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-1} \phi(p_1 p_2 \cdots p_{r-1}) = \phi\left(\frac{n}{p_r^{n_r}}\right) p_r^{n_r-1}. \end{aligned}$$

The last part of the lemma can be seen easily. Note that $\phi(p_r) > p_i$ for $r \geq 3$. □

Lemma 2.2. *We have $\phi(p_1 p_2 \cdots p_t) - p_1 p_2 \cdots p_t + \sum_{k=1}^t \frac{p_1 p_2 \cdots p_t}{p_k} \geq 0$ for all $t \geq 1$. Further, equality holds if and only if $t = 1$.*

Proof. Clearly, equality holds if $t = 1$. The rest follows using induction on $t \geq 2$. □

For $x \in C_n$, we denote by $o(x)$ the order of x . If two elements x, y are adjacent in $\mathcal{P}(C_n)$, then $o(x) \mid o(y)$ or $o(y) \mid o(x)$ according as $x \in \langle y \rangle$ or $y \in \langle x \rangle$. The converse statement is also true (which does not hold for an arbitrary finite group), follows from the properties of a finite cyclic group. We shall use this fact frequently without mention. For $x \in C_n$, let $N(x)$ be the neighborhood of x in $\mathcal{P}(C_n)$, that is, the set of all elements of C_n which are adjacent to x . If $o(x) = o(y)$ for $x, y \in C_n$, then it is clear that $N(x) \cup \{x\} = N(y) \cup \{y\}$, also see [7, Lemma 3].

Let X be a subset of C_n . For two disjoint nonempty subsets A and B of \overline{X} , we say that $A \cup B$ is a *separation* of $\mathcal{P}(\overline{X})$ if $\overline{X} = A \cup B$ and there is no edge containing vertices from both A and B . Thus $\mathcal{P}(\overline{X})$ is disconnected if and only if there exists a separation of it. For a positive divisor d of n , we define the following two sets:

E_d = the set of all elements of C_n whose order is d ,

S_d = the set of all elements of C_n whose order divides d .

Then S_d is a cyclic subgroup of C_n of order d and E_d is precisely the set of generators of S_d . So $|S_d| = d$ and $|E_d| = \phi(d)$. The following result is very useful throughout the paper.

Lemma 2.3. *Let X be a subset of C_n of minimum possible size with the property that $\mathcal{P}(\overline{X})$ is disconnected. Then either $E_d \subseteq X$ or $E_d \cap X$ is empty for each divisor d of n .*

Proof. Suppose that $E_d \cap X \neq \emptyset$. We show that $E_d \subseteq X$. Fix a separation $A \cup B$ of $\mathcal{P}(\overline{X})$. Let $x \in E_d \cap X$. The minimality of $|X|$ implies that the subgraph $\mathcal{P}(\overline{X} \setminus \{x\})$ of $\mathcal{P}(C_n)$ is connected. So there exist $a \in A$ and $b \in B$ such that x is adjacent to both a and b .

Suppose that there exists an element $y \in E_d$ which is not in X . Then $y \neq x$. Since $o(x) = o(y) = d$, we have $N(x) \cup \{x\} = N(y) \cup \{y\}$. If $y \in A$ (respectively, $y \in B$), then the fact that x is adjacent to b (respectively, to a) implies y is adjacent to b (respectively, to a). This contradicts that $A \cup B$ is a separation of $\mathcal{P}(\overline{X})$. \square

Remark 2.4. Under the hypothesis of Lemma 2.3, it follows that there are three possibilities for the set E_d , where d is a divisor of n : either $E_d \subseteq X$, $E_d \subseteq A$ or $E_d \subseteq B$, where $A \cup B$ is any separation of $\mathcal{P}(\overline{X})$.

We complete this section with the following lemma. For a given subset $\{i_1, i_2, \dots, i_k\}$ of $\{1, 2, \dots, r\}$, we define the integer m_{i_1, i_2, \dots, i_k} by

$$m_{i_1, i_2, \dots, i_k} = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}.$$

Lemma 2.5. $\kappa(\mathcal{P}(C_n)) = \phi(n) + 1$ if and only if $r = 2$ and $n = p_1 p_2$.

Proof. If $n = p_1 p_2$, then $\kappa(\mathcal{P}(C_n)) = \phi(n) + 1$ by [4, Theorem 3(ii)]. For the converse part, let $X = E_1 \cup E_n$. It is enough to show that $\mathcal{P}(\overline{X})$ is connected whenever $r \geq 3$, or $r = 2$ and one of n_1, n_2 is at least 2.

Let x and y be two distinct elements of \overline{X} . Then $x \in S_{m_j}$ and $y \in S_{m_k}$ for some $j, k \in \{1, 2, \dots, r\}$. So x (respectively, y) is adjacent with the elements of $E_{m_j} \setminus \{x\}$ (respectively, $E_{m_k} \setminus \{y\}$). If $j = k$, then x and y are connected through the elements of E_{m_j} . Assume that $j \neq k$. Since $r \geq 3$, or $r = 2$ and one of n_1, n_2 is at least 2, the set $E_{m_{j,k}}$ is non-empty. Then the elements of both E_{m_j} and E_{m_k} are adjacent with the elements of $E_{m_{j,k}}$. It follows that x and y are connected by a path. \square

3 Upper bounds and Proof of Theorem 1.1(ii) and (iii)

We shall prove the bounds in Theorem 1.1 by identifying suitable subsets X of C_n of required size such that $\mathcal{P}(\overline{X})$ is disconnected. Let $0 \leq k \leq n_r - 1$. Define the following integers:

$$\alpha_k = p_1^{n_1} p_2^{n_2} \cdots p_{r-1}^{n_{r-1}} p_r^k.$$

So $\alpha_k = \alpha_0 p_r^k$. For given k and subset $\{i_1, i_2, \dots, i_l\}$ of $\{1, 2, \dots, r-1\}$, define the integer $\beta_{k, i_1, i_2, \dots, i_l}$ by

$$\beta_{k, i_1, i_2, \dots, i_l} = \frac{\alpha_k}{p_{i_1} \cdots p_{i_l}} = \frac{p_1^{n_1} \cdots p_{r-1}^{n_{r-1}} p_r^k}{p_{i_1} \cdots p_{i_l}}.$$

Set

$$Z(r, k) = E_{\alpha_{k+1}} \cup \cdots \cup E_{\alpha_{n_r-1}} \cup E_n \cup S_{\beta_{k,1}} \cup \cdots \cup S_{\beta_{k, r-1}}.$$

Proposition 3.1. The subgraph $\mathcal{P}(\overline{Z(r, k)})$ of $\mathcal{P}(C_n)$ is disconnected.

Proof. For $x \in \overline{Z(r, k)}$, observe that the order $o(x)$ of x is one of the following two types:

- (I) $o(x) = p_1^{n_1} p_2^{n_2} \cdots p_{r-1}^{n_{r-1}} p_r^s$, where $0 \leq s \leq k$;
- (II) $o(x) = p_1^{l_1} \cdots p_{r-1}^{l_{r-1}} p_r^t$, where $k+1 \leq t \leq n_r$, $0 \leq l_i \leq n_i$ for $i \in \{1, \dots, r-1\}$ and $(l_1, \dots, l_{r-1}) \neq (n_1, \dots, n_{r-1})$.

Let A (respectively, B) be the subset of $\overline{Z(r, k)}$ consisting of all the elements whose order is of type (I) (respectively, of type (II)). Then A, B are nonempty sets and $\overline{Z(r, k)} = A \cup B$ is a disjoint union. Since $t > s$, no element of B can be obtained as an integral power of any element of A . Again, since $(l_1, \dots, l_{r-1}) \neq (n_1, \dots, n_{r-1})$, no element of A can be obtained as an integral power of any element of B . It follows that $A \cup B$ is a separation of $\mathcal{P}(\overline{Z(r, k)})$. \square

Proposition 3.2. *The number of elements in $Z(r, k)$ is given by:*

$$|Z(r, k)| = \phi(n) + \beta_{0,1,\dots,r-1} \left[p_r^{n_r-1} \phi(p_1 \cdots p_{r-1}) + p_r^k [p_1 \cdots p_{r-1} - 2\phi(p_1 \cdots p_{r-1})] \right].$$

Proof. The sets $E_{\alpha_{k+1}}, \dots, E_{\alpha_{n_r-1}}, E_n$ are pairwise disjoint and each of them is disjoint from $\bigcup_{i=1}^{r-1} S_{\beta_{k,i}}$. So

$$|Z(r, k)| = |E_n| + \bigcup_{i=k+1}^{n_r-1} |E_{\alpha_i}| + \left| \bigcup_{i=1}^{r-1} S_{\beta_{k,i}} \right|.$$

We have

$$\begin{aligned} \bigcup_{i=k+1}^{n_r-1} |E_{\alpha_i}| &= \phi(\alpha_0) \left[\phi(p_r^{k+1}) + \phi(p_r^{k+2}) + \cdots + \phi(p_r^{n_r-1}) \right] \\ &= p_1^{n_1-1} p_2^{n_2-1} \cdots p_{r-1}^{n_{r-1}-1} \phi(p_1 p_2 \cdots p_{r-1}) (p_r^{n_r-1} - p_r^k). \end{aligned}$$

and

$$\begin{aligned} \left| \bigcup_{i=1}^{r-1} S_{\beta_{k,i}} \right| &= \sum_i |S_{\beta_{k,i}}| - \sum_{i < j} |S_{\beta_{k,i}} \cap S_{\beta_{k,j}}| + \cdots + (-1)^{r-2} |S_{\beta_{k,1}} \cap \cdots \cap S_{\beta_{k,r-1}}| \\ &= \sum_i \beta_{k,i} - \sum_{i < j} \beta_{k,i,j} + \cdots + (-1)^{r-2} \beta_{k,1,2,\dots,r-1} \\ &= p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^k \left[\sum_{i=1}^{r-1} \frac{p_1 \cdots p_{r-1}}{p_i} - \sum_{i < j} \frac{p_1 \cdots p_{r-1}}{p_i p_j} + \cdots + (-1)^{r-2} \right] \\ &= p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^k [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})]. \end{aligned}$$

Now the lemma follows from the above, as $\beta_{0,1,\dots,r-1} = p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1}$. \square

In the next section, we shall have occasions to calculate the cardinality of the union of certain subgroups, which will be similar to that of calculating $\left| \bigcup_{i=1}^{r-1} S_{\beta_{k,i}} \right|$ as in the above. As a consequence of Propositions 3.1 and 3.2, we have the following.

Corollary 3.3. *The vertex connectivity $\kappa(\mathcal{P}(C_n))$ of $\mathcal{P}(C_n)$ satisfies the following:*

$$\kappa(\mathcal{P}(C_n)) \leq \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} \left[p_r^{n_r-1} \phi(p_1 \cdots p_{r-1}) + p_r^k [p_1 \cdots p_{r-1} - 2\phi(p_1 \cdots p_{r-1})] \right].$$

Proof of Theorem 1.1(ii). If $2\phi(p_1 \cdots p_{r-1}) < p_1 \cdots p_{r-1}$, then the minimum of $|Z(r, k)|$ occurs when $k = 0$. This gives

$$\kappa(\mathcal{P}(C_n)) \leq \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} [p_1 \cdots p_{r-1} + \phi(p_1 \cdots p_{r-1})(p_r^{n_r-1} - 2)], \quad (2)$$

thus proving Theorem 1.1(ii). \square

If $2\phi(p_1 \cdots p_{r-1}) > p_1 \cdots p_{r-1}$, then the minimum of $|Z(r, k)|$ occurs when $k = n_r - 1$ and this gives

$$\kappa(\mathcal{P}(C_n)) \leq \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})]. \quad (3)$$

In the next section, we shall show that equality holds in (3) which will prove Theorem 1.1(i). Observe that the bounds (2) and (3) coincide if $n_r = 1$, or if $r = 2$ and $p_1 = 2$.

Proof of Theorem 1.1(iii). Note that $2\phi(p_1 \cdots p_{r-1}) = p_1 \cdots p_{r-1}$ if and only if $r = 2$ and $p_1 = 2$. So $n = 2^{n_1} p_2^{n_2}$ in this case. For $r = 2$ and $0 \leq k \leq n_2 - 1$, we have

$$Z(2, k) = E_{2^{n_1} p_2^{k+1}} \cup E_{2^{n_1} p_2^{k+2}} \cup \cdots \cup E_{2^{n_1} p_2^{n_2-1}} \cup E_n \cup S_{2^{n_1-1} p_2^k}$$

and that $|Z(2, k)| = \phi(n) + 2^{n_1-1} p_2^{n_2-1}$ is independent of k . Thus

$$\kappa(\mathcal{P}(C_n)) \leq |Z(2, k)| = \phi(n) + 2^{n_1-1} p_2^{n_2-1}.$$

Now, let X be a subset of C_n of minimum possible size such that $\mathcal{P}(\overline{X})$ is disconnected. In order to prove Theorem 1.1(iii), it is enough to show that $X = Z(2, t)$ for some $0 \leq t \leq n_2 - 1$. Write $T = X \setminus (E_1 \cup E_n)$. Since X contains $E_1 \cup E_n$ and $|X| \leq \phi(n) + 2^{n_1-1} p_2^{n_2-1}$, we get

$$|T| \leq 2^{n_1-1} p_2^{n_2-1} - 1.$$

We claim that the set $E_{2^{n_1-1} p_2^{n_2}}$ is disjoint from X . Otherwise, $E_{2^{n_1-1} p_2^{n_2}} \subseteq T$ by Lemma 2.3 and so $|E_{2^{n_1-1} p_2^{n_2}}| \leq |T|$. On the other hand, using Lemma 2.1, we get

$$|E_{2^{n_1-1} p_2^{n_2}}| = \phi(2^{n_1-1} p_2^{n_2}) \geq \phi(2^{n_1}) p_2^{n_2-1} > 2^{n_1-1} p_2^{n_2-1} - 1 \geq |T|,$$

a contradiction.

Let $A \cup B$ be a separation of $\mathcal{P}(\overline{X})$. We may assume that $E_{2^{n_1-1} p_2^{n_2}}$ is contained in B . Then, for $x \in A$, we must have

$$o(x) = 2^{n_1} p_2^j$$

for some j with $0 \leq j \leq n_2 - 1$. Let $t \in \{0, 1, \dots, n_2 - 1\}$ be the largest integer for which A has an element of order $2^{n_1} p_2^t$. Then, using Lemma 2.3 together with the fact that $A \cup B$ is a separation of $\mathcal{P}(\overline{X})$, the following hold:

- (i) $E_{2^{n_1} p_2^t} \subseteq A$,
- (ii) $E_{2^{n_1} p_2^{t+1}}, E_{2^{n_1} p_2^{t+2}}, \dots, E_{2^{n_1} p_2^{n_2-1}}$ are contained in T ,
- (iii) the subgroup $S_{2^{n_1-1} p_2^t}$ is contained in X .

Thus X contains $Z(2, t)$. Since $|X| \leq \phi(n) + 2^{n_1-1} p_2^{n_2-1} = |Z(2, t)|$, it follows that $X = Z(2, t)$. This completes the proof. \square

4 Proof of Theorem 1.1(i) and Corollary 1.2

Assume, throughout this section, that $2\phi(p_1 \cdots p_{r-1}) > p_1 \cdots p_{r-1}$ (and so $p_1 \geq 3$). Let X be a subset of C_n of minimum possible size with the property that $\mathcal{P}(\overline{X})$ is disconnected. By (3),

$$|X| \leq \phi(n) + p_1^{n_1-1} p_2^{n_2-1} \cdots p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})].$$

Set $T = X \setminus E_n$. Since $E_n \subseteq X$, we have

$$|T| \leq p_1^{n_1-1} p_2^{n_2-1} \cdots p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})]. \quad (4)$$

Proposition 4.1. *Each of the sets E_{m_i} , $1 \leq i \leq r-1$, is disjoint from X .*

Proof. Suppose that $E_{m_i} \cap X \neq \emptyset$. Then $E_{m_i} \subseteq X$ by Lemma 2.3, in fact, $E_{m_i} \subseteq T$. So $|E_{m_i}| \leq |T|$. Since $1 \leq i \leq r-1$, $|E_{m_i}| = \phi\left(\frac{n}{p_i}\right) > \phi\left(\frac{n}{p_r}\right) p_r^{n_r-1}$ by Lemma 2.1 and so

$$|E_{m_i}| > p_1^{n_1-1} p_2^{n_2-1} \cdots p_r^{n_r-1} \phi(p_1 p_2 \cdots p_{r-1}). \quad (5)$$

Then the inequalities (4) and (5) together imply

$$|E_{m_i}| - |T| > p_1^{n_1-1} p_2^{n_2-1} \cdots p_r^{n_r-1} [2\phi(p_1 p_2 \cdots p_{r-1}) - p_1 p_2 \cdots p_{r-1}].$$

Since $2\phi(p_1 p_2 \cdots p_{r-1}) > p_1 p_2 \cdots p_{r-1}$, it follows that $|E_{m_i}| > |T|$, a contradiction. \square

We shall prove later that the set E_{m_r} is also disjoint from X . However, the argument used in the proof of Proposition 4.1 can not be applied (when $n_r \geq 2$) to prove this statement.

Fix a separation $A \cup B$ of $\mathcal{P}(\overline{X})$. Proposition 4.1 implies that each E_{m_i} , $1 \leq i \leq r-1$, is contained either in A or in B .

Proposition 4.2. *Suppose that $r \geq 3$. If $E_{m_i} \subseteq A$ and $E_{m_j} \subseteq B$ for some $1 \leq i \neq j \leq r-1$, then E_{m_r} is disjoint from X .*

Proof. Since $A \cup B$ is a separation of $\mathcal{P}(\overline{X})$, the subgroup $S_{m_{i,j}}$ of C_n is contained in T . Suppose that $E_{m_r} \cap X \neq \emptyset$. Then $E_{m_r} \subseteq T$ by Lemma 2.3. So $|S_{m_{i,j}}| + |E_{m_r}| = |S_{m_{i,j}} \cup E_{m_r}| \leq |T|$. If $n_r \geq 2$, then

$$\begin{aligned} |S_{m_{i,j}}| + |E_{m_r}| &= \frac{n}{p_i p_j} + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-2} \phi(p_1 p_2 \cdots p_r) \\ &= p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-2} \left(p_r^2 \prod_{\substack{k=1 \\ k \neq i,j}}^{r-1} p_k + \phi(p_1 \cdots p_r) \right) \\ &> p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-2} \left(\prod_{k=1}^{r-1} p_k + \phi(p_1 \cdots p_r) \right), \end{aligned}$$

and so

$$\begin{aligned} \frac{|S_{m_{i,j}}| + |E_{m_r}| - |T|}{p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-2}} &> \prod_{k=1}^{r-1} p_k + \phi(p_1 \cdots p_r) - p_r \left[\prod_{k=1}^{r-1} p_k - \phi(p_1 \cdots p_{r-1}) \right] \\ &= \prod_{k=1}^{r-1} p_k + \phi(p_1 \cdots p_{r-1})(p_r - 1) - p_r \left[\prod_{k=1}^{r-1} p_k - \phi(p_1 \cdots p_{r-1}) \right] \\ &= \prod_{k=1}^{r-1} p_k - \phi(p_1 \cdots p_{r-1}) + p_r \left[2\phi(p_1 \cdots p_{r-1}) - \prod_{k=1}^{r-1} p_k \right] > 0. \end{aligned}$$

If $n_r = 1$, then $|S_{m_{i,j}}| + |E_{m_r}| = \frac{n}{p_i p_j} + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} \phi(p_1 p_2 \cdots p_{r-1})$ and so

$$\frac{|S_{m_{i,j}}| + |E_{m_r}| - |T|}{p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1}} \geq \prod_{\substack{k=1 \\ k \neq i,j}}^r p_k + 2\phi(p_1 \cdots p_{r-1}) - p_1 p_2 \cdots p_{r-1} > 0.$$

In both cases, it follows that $|S_{m_{i,j}}| + |E_{m_r}| > |T|$, a contradiction. \square

Proposition 4.3. *All the sets E_{m_i} , $1 \leq i \leq r-1$, are contained either in A or in B .*

Proof. Clearly, this holds for $r = 2$. Assume that $r \geq 3$. Suppose that some of the sets E_{m_i} , $1 \leq i \leq r-1$, are contained in A and some are in B . Then E_{m_r} is disjoint from X by Proposition 4.2. Without loss, we may assume that E_{m_r} is contained in A . Let

$$a = |\{E_{m_i} : 1 \leq i \leq r-1, E_{m_i} \subseteq A\}|$$

Then $1 \leq a \leq r-2$ by our assumption. We shall get a contradiction by showing that $a \notin \{1, 2, \dots, r-2\}$.

Claim-1: $a \neq r-2$. Suppose that $a = r-2$. Let $E_{m_{i_1}}, E_{m_{i_2}}, \dots, E_{m_{i_a}}$ be the sets contained in A and $E_{m_{i_{a+1}}}$ be contained in B , where $\{i_1, \dots, i_a, i_{a+1}\} = \{1, 2, \dots, r-1\}$. Since E_{m_r} is contained in A , the subgroups

$$S_{m_r, i_{a+1}}, S_{m_{i_1}, i_{a+1}}, S_{m_{i_2}, i_{a+1}}, \dots, S_{m_{i_a}, i_{a+1}}$$

are contained in T . This follows as $A \cup B$ is a separation of $\mathcal{P}(\overline{X})$. Let Q be the union of these $r-1$ subgroups. Then $|Q| \leq |T|$. We shall get a contradiction by showing that $|Q| > |T|$.

The subscript i_{a+1} is common to all the above $r-1$ subgroups. Applying a similar calculation as in the proof of Proposition 3.2, we get

$$\begin{aligned} |Q| &= p_{i_1}^{n_{i_1}-1} \cdots p_{i_a}^{n_{i_a}-1} p_{i_{a+1}}^{n_{i_{a+1}}-1} p_r^{n_r-1} [p_{i_1} \cdots p_{i_a} p_r - \phi(p_{i_1} \cdots p_{i_a} p_r)] \\ &= p_1^{n_1-1} p_2^{n_2-1} \cdots p_r^{n_r-1} [p_{i_1} \cdots p_{i_a} p_r - \phi(p_{i_1} \cdots p_{i_a} p_r)]. \end{aligned}$$

Then

$$\begin{aligned} \frac{|Q| - |T|}{p_1^{n_1-1} \cdots p_r^{n_r-1}} &\geq p_{i_1} \cdots p_{i_a} p_r - \phi(p_{i_1} \cdots p_{i_a} p_r) - p_1 p_2 \cdots p_{r-1} + \phi(p_1 p_2 \cdots p_{r-1}) \\ &= p_{i_1} \cdots p_{i_a} (p_r - p_{i_{a+1}}) + \phi(p_{i_1} \cdots p_{i_a}) [\phi(p_{i_{a+1}}) - \phi(p_r)] \\ &= (p_r - p_{i_{a+1}})(p_{i_1} \cdots p_{i_a} - \phi(p_{i_1} \cdots p_{i_a})) > 0. \end{aligned}$$

The last inequality holds as $1 \leq i_{a+1} \leq r-1$. So $|Q| > |T|$, a contradiction. This proves Claim-1.

Claim-2: $a \notin \{1, 2, \dots, r-3\}$. Suppose that $1 \leq a \leq r-3$ (we must have $r \geq 4$ as $a \geq 1$). Set $b = r-1-a$. Then $b \geq 2$. Let $E_{m_{i_1}}, \dots, E_{m_{i_a}}$ be the sets contained in A and $E_{m_{i_{a+1}}}, E_{m_{i_{a+2}}}, \dots, E_{m_{i_{a+b}}}$ be contained in B , where

$$\{i_1, \dots, i_a, i_{a+1}, \dots, i_{a+b}\} = \{1, 2, \dots, r-1\}.$$

So the following subgroups

$$\begin{aligned} &S_{m_r, i_{a+1}}, S_{m_r, i_{a+2}}, \dots, S_{m_r, i_{a+b}} \\ &S_{m_{i_1}, i_{a+1}}, S_{m_{i_1}, i_{a+2}}, \dots, S_{m_{i_1}, i_{a+b}} \\ &\vdots \\ &S_{m_{i_a}, i_{a+1}}, S_{m_{i_a}, i_{a+2}}, \dots, S_{m_{i_a}, i_{a+b}} \end{aligned}$$

are contained in T . Let $1 \leq s \leq a$ and $1 \leq t \leq b$. Note that $E_{m_{i_s}, i_{a+t}}$ is the set of generators of the subgroup $S_{m_{i_s}, i_{a+t}}$ and so is contained in T . Define the set

$$R = \left(\bigcup_{j=1}^b S_{m_r, i_{a+j}} \right) \cup \left(\bigcup_{t=1}^b \left(\bigcup_{s=1}^a E_{m_{i_s}, i_{a+t}} \right) \right).$$

Since R is contained in T , we have $|R| \leq |T|$. We shall get a contradiction by showing that $|R| > |T|$.

The subscript r is common to all the b subgroups contained in R . Applying a similar calculation as in the proof of Proposition 3.2, we have

$$\begin{aligned} \left| \bigcup_{j=1}^b S_{m_r, i_{a+j}} \right| &= p_{i_1}^{n_{i_1}} \cdots p_{i_a}^{n_{i_a}} p_{i_{a+1}}^{n_{i_{a+1}}-1} \cdots p_{i_{a+b}}^{n_{i_{a+b}}-1} p_r^{n_r-1} [p_{i_{a+1}} \cdots p_{i_{a+b}} - \phi(p_{i_{a+1}} \cdots p_{i_{a+b}})] \\ &= p_{i_1}^{n_{i_1}-1} \cdots p_{i_{a+b}}^{n_{i_{a+b}}-1} p_r^{n_r-1} [p_{i_1} \cdots p_{i_a} p_{i_{a+1}} \cdots p_{i_{a+b}} - p_{i_1} \cdots p_{i_a} \phi(p_{i_{a+1}} \cdots p_{i_{a+b}})] \\ &= p_1^{n_1-1} p_2^{n_2-1} \cdots p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - p_{i_1} \cdots p_{i_a} \phi(p_{i_{a+1}} \cdots p_{i_{a+b}})]. \end{aligned}$$

We next calculate a lower bound for $|E_{m_{i_s}, i_{a+t}}|$. Applying Lemma 2.1,

$$\phi \left(\frac{p_{i_{a+1}}^{n_{i_{a+1}}} \cdots p_{i_{a+b}}^{n_{i_{a+b}}} p_r^{n_r}}{p_{i_{a+t}}} \right) > p_{i_{a+1}}^{n_{i_{a+1}}-1} \cdots p_{i_{a+b}}^{n_{i_{a+b}}-1} p_r^{n_r-1} \times \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}). \quad (6)$$

It can easily be seen (irrespective of $n_{i_s} = 1$ or $n_{i_s} \geq 2$) that

$$\phi \left(\frac{p_{i_1}^{n_{i_1}} \cdots p_{i_a}^{n_{i_a}}}{p_{i_s}} \right) \geq p_{i_1}^{n_{i_1}-1} \cdots p_{i_a}^{n_{i_a}-1} \times \frac{\phi(p_{i_1} p_{i_2} \cdots p_{i_a})}{p_{i_s}}. \quad (7)$$

Using the inequalities (6) and (7), we get

$$\begin{aligned} |E_{m_{i_s}, i_{a+t}}| &= \phi \left(\frac{n}{p_{i_s} p_{i_{a+t}}} \right) \\ &= \phi \left(\frac{p_{i_1}^{n_{i_1}} \cdots p_{i_a}^{n_{i_a}}}{p_{i_s}} \right) \phi \left(\frac{p_{i_{a+1}}^{n_{i_{a+1}}} \cdots p_{i_{a+b}}^{n_{i_{a+b}}} p_r^{n_r}}{p_{i_{a+t}}} \right) \\ &> p_1^{n_1-1} \cdots p_r^{n_r-1} \times \frac{\phi(p_{i_1} p_{i_2} \cdots p_{i_a})}{p_{i_s}} \times \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}). \end{aligned}$$

So

$$\sum_{s=1}^a |E_{m_{i_s}, i_{a+t}}| > p_1^{n_1-1} \cdots p_r^{n_r-1} \times \left(\sum_{s=1}^a \frac{\phi(p_{i_1} p_{i_2} \cdots p_{i_a})}{p_{i_s}} \right) \times \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}). \quad (8)$$

Observe that the right hand side of (8) is independent of t . Since $b \geq 2$ and the sets $E_{m_{i_s}, i_{a+t}}$ are pairwise disjoint, we get

$$\begin{aligned} \left| \bigcup_{t=1}^b \left(\bigcup_{s=1}^a E_{m_{i_s}, i_{a+t}} \right) \right| &= \sum_{t=1}^b \left(\sum_{s=1}^a |E_{m_{i_s}, i_{a+t}}| \right) = b \times \left(\sum_{s=1}^a |E_{m_{i_s}, i_{a+t}}| \right) \\ &> 2 p_1^{n_1-1} \cdots p_r^{n_r-1} \left(\sum_{s=1}^a \frac{\phi(p_{i_1} p_{i_2} \cdots p_{i_a})}{p_{i_s}} \right) \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}) \\ &= p_1^{n_1-1} \cdots p_r^{n_r-1} \left(\sum_{s=1}^a \frac{2 \phi(p_{i_1} p_{i_2} \cdots p_{i_a})}{p_{i_s}} \right) \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}) \\ &> p_1^{n_1-1} \cdots p_r^{n_r-1} \left(\sum_{s=1}^a \frac{p_{i_1} p_{i_2} \cdots p_{i_a}}{p_{i_s}} \right) \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}). \end{aligned}$$

The hypothesis that $2\phi(p_1 \cdots p_{r-1}) > p_1 \cdots p_{r-1}$ implies $2\phi(p_{j_1} \cdots p_{j_l}) > p_{j_1} \cdots p_{j_l}$ for any subset $\{j_1, \dots, j_l\}$ of $\{1, 2, \dots, r-1\}$. So the last inequality holds in the above. Note that each of the sets $E_{m_{i_s}, i_{a+t}}$ is disjoint from $\bigcup_{j=1}^b S_{m_r, i_{a+j}}$. So

$$|R| - |T| = \left| \bigcup_{j=1}^b S_{m_r, i_{a+j}} \right| + \left| \bigcup_{t=1}^b \left(\bigcup_{s=1}^a E_{m_{i_s}, i_{a+t}} \right) \right| - |T|.$$

Then

$$\begin{aligned} \frac{|R| - |T|}{p_1^{n_1-1} \cdots p_r^{n_r-1}} &> \phi(p_1 p_2 \cdots p_{r-1}) - p_{i_1} \cdots p_{i_a} \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}) \\ &\quad + \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}) \left(\sum_{s=1}^a \frac{p_{i_1} p_{i_2} \cdots p_{i_a}}{p_{i_s}} \right) \\ &= \phi(p_{i_{a+1}} \cdots p_{i_{a+b}}) \left[\phi(p_{i_1} \cdots p_{i_a}) - p_{i_1} \cdots p_{i_a} + \left(\sum_{s=1}^a \frac{p_{i_1} \cdots p_{i_a}}{p_{i_s}} \right) \right] \\ &\geq 0. \end{aligned}$$

The last inequality holds by Lemma 2.2. It follows that $|R| > |T|$, a contradiction. This proves Claim-2. \square

The following proves Theorem 1.1(i). Recall the integers α_k and $\beta_{k, i_1, i_2, \dots, i_l}$ defined in Section 3 for $0 \leq k \leq n_r - 1$ and subsets $\{i_1, i_2, \dots, i_l\}$ of $\{1, 2, \dots, r-1\}$.

Proposition 4.4. *The set E_{m_r} is disjoint from X . As a consequence, $X = Z(r, n_r - 1)$ and*

$$\kappa(\mathcal{P}(C_n)) = \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})].$$

Proof. By Proposition 4.3, we may assume that all the sets E_{m_i} , $1 \leq i \leq r-1$, are contained in B . We show that E_{m_r} is contained in A .

Note that the order of an element in A is of the form $\alpha_j = p_1^{n_1} p_2^{n_2} \cdots p_{r-1}^{n_{r-1}} p_r^j$ for some j with $0 \leq j \leq n_r - 1$. This follows, since the elements of A are not adjacent with the elements of E_{m_i} , $1 \leq i \leq r-1$, in B . Let $t \in \{0, 1, \dots, n_r - 1\}$ be the largest integer for which A has an element of order α_t . Then Lemma 2.3 implies that $E_{\alpha_t} \subseteq A$. We claim that $t = n_r - 1$.

If $n_r = 1$, then there is nothing to prove. So consider $n_r \geq 2$. Suppose that $t < n_r - 1$. Since $A \cup B$ is a separation of $\mathcal{P}(\overline{X})$, the sets E_{α_k} ($t+1 \leq k \leq n_r - 1$) and the subgroups $S_{\beta_{t,l}}$ ($1 \leq l \leq r-1$) are contained in T . Set

$$P = \bigcup_{k=t+1}^{n_r-1} E_{\alpha_k} \text{ and } Q = \bigcup_{l=1}^{r-1} S_{\beta_{t,l}}.$$

Then $|P| + |Q| = |P \cup Q| \leq |T|$. We now calculate $|P|$ and $|Q|$. Since the sets E_{α_k} are pairwise disjoint, we have

$$\begin{aligned} |P| &= |E_{\alpha_{t+1}}| + |E_{\alpha_{t+2}}| + \cdots + |E_{\alpha_{n_r-1}}| \\ &= \phi(p_1^{n_1} p_2^{n_2} \cdots p_{r-1}^{n_{r-1}}) \sum_{k=t+1}^{n_r-1} \phi(p_r^k) \\ &= p_1^{n_1-1} p_2^{n_2-1} \cdots p_{r-1}^{n_{r-1}-1} \phi(p_1 p_2 \cdots p_{r-1}) (p_r^{n_r-1} - p_r^t). \end{aligned}$$

Applying a similar calculation as in the proof of Proposition 3.2, we get

$$|Q| = p_1^{n_1-1} p_2^{n_2-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^t [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})].$$

Then

$$\begin{aligned} \frac{|P| + |Q| - |T|}{p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1}} &\geq \phi(p_1 \cdots p_{r-1}) (p_r^{n_r-1} - p_r^t) \\ &\quad - [p_1 \cdots p_{r-1} - \phi(p_1 \cdots p_{r-1})] (p_r^{n_r-1} - p_r^t) \\ &= [2\phi(p_1 \cdots p_{r-1}) - p_1 \cdots p_{r-1}] (p_r^{n_r-1} - p_r^t) > 0. \end{aligned}$$

The last inequality holds, since $0 \leq t < n_r - 1$ and $2\phi(p_1 \cdots p_{r-1}) > p_1 \cdots p_{r-1}$. It follows that $|P| + |Q| > |T|$, a contradiction. Hence $t = n_r - 1$ and E_{m_r} is contained in A .

We now show that $X = Z(r, n_r - 1)$. Since E_{m_r} is contained in A and E_{m_i} , $1 \leq i \leq r - 1$, are contained in B , the subgroups

$$S_{m_{1,r}}, S_{m_{2,r}}, \cdots, S_{m_{r-1,r}}$$

of C_n must be contained in X . Since $E_n \subseteq X$, it follows that X contains $Z(r, n_r - 1)$. Then minimality of $|X|$ implies that $X = Z(r, n_r - 1)$ and so

$$\kappa(\mathcal{P}(C_n)) = |Z(r, n_r - 1)| = \phi(n) + p_1^{n_1-1} \cdots p_{r-1}^{n_{r-1}-1} p_r^{n_r-1} [p_1 p_2 \cdots p_{r-1} - \phi(p_1 p_2 \cdots p_{r-1})].$$

This completes the proof. \square

As a consequence of Theorem 1.1(i) and (iii), we now prove Corollary 1.2.

Proof of Corollary 1.2. Since $p_1 \geq r \geq 2$, we get

$$\begin{aligned} \frac{\phi(p_1 p_2 \cdots p_{r-1})}{p_1 p_2 \cdots p_{r-1}} &= \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_{r-1}}\right) \\ &\geq \left(1 - \frac{1}{r}\right) \left(1 - \frac{1}{r+1}\right) \cdots \left(1 - \frac{1}{2(r-1)}\right) = \frac{1}{2}, \end{aligned}$$

where the inequality is strict except when $r = 2$ and $p_1 = 2$. Thus $2\phi(p_1 \cdots p_{r-1}) \geq p_1 \cdots p_{r-1}$, with equality if and only if $(r, p_1) = (2, 2)$. Then the corollary follows from Theorem 1.1(i) and (iii). \square

5 Proof of Theorem 1.3

Here $r = 3$. Since $2\phi(p_1 p_2) < p_1 p_2$, it follows from the proof Corollary 1.2 that $p_1 < 3 = r$. So $p_1 = 2$ and $n = 2^{n_1} p_2^{n_2} p_3^{n_3}$. Since $2 < p_2 < p_3$, we have $p_2 \geq 3$ and $p_3 \geq 5$. Let X be a subset of C_n of minimum size such that $\mathcal{P}(\overline{X})$ is disconnected. Then, using the bound (2), we have $|X| \leq \phi(n) + 2^{n_1-1} p_2^{n_2-1} [p_3^{n_3-1} \phi(p_2) + 2]$. Setting $\Gamma = X \setminus E_n$, we get

$$|\Gamma| \leq 2^{n_1-1} p_2^{n_2-1} [p_3^{n_3-1} \phi(p_2) + 2]. \quad (9)$$

Proposition 5.1. E_{m_1} is disjoint from X .

Proof. Otherwise, $E_{m_1} \subseteq \Gamma$ by Lemma 2.3. Since the identity element of C_n is in Γ but not in E_{m_1} , we get $|E_{m_1}| < |\Gamma|$. On the other hand, using (9), we have

$$|E_{m_1}| - |\Gamma| \geq \begin{cases} p_2^{n_2-1} [p_3^{n_3-1} (p_2 - 1)(p_3 - 2) - 2], & \text{if } n_1 = 1 \\ 2^{n_1-2} p_2^{n_2-1} [p_3^{n_3-1} (p_2 - 1)(p_3 - 3) - 4], & \text{if } n_1 \geq 2 \end{cases}.$$

Since $p_2 \geq 3$ and $p_3 \geq 5$, it follows that $|E_{m_1}| - |\Gamma| \geq 0$, a contradiction. \square

Fix a separation $A \cup B$ of $\mathcal{P}(\overline{X})$. By the above proposition, E_{m_1} is contained either in A or in B . Without loss of generality, we may assume that $E_{m_1} \subseteq A$.

Proposition 5.2. *At least one of E_{m_2} and E_{m_3} is disjoint from X .*

Proof. Otherwise, both E_{m_2} and E_{m_3} are contained in Γ by Lemma 2.3 and so $|E_{m_2}| + |E_{m_3}| \leq |\Gamma|$. Set $\theta = |E_{m_2}| + |E_{m_3}| - |\Gamma|$. Using (9), the following can be verified:

$$\theta \geq \begin{cases} 2^{n_1-1}(p_3 - 3), & \text{if } n_2 = 1 = n_3 \\ 2^{n_1-1} \left(p_3^{n_3-2} [p_3(p_3 - p_2) + \phi(p_2 p_3)] - 2 \right), & \text{if } n_2 = 1 \text{ and } n_3 \geq 2 \\ 2^{n_1-1} p_2^{n_2-2} (\phi(p_2 p_3) - 2p_2), & \text{if } n_2 \geq 2 \text{ and } n_3 = 1 \\ 2^{n_1-1} p_2^{n_2-2} \left(p_3^{n_3-2} \phi(p_2) (p_3^2 - p_3 - p_2) - 2p_2 \right), & \text{if } n_2 \geq 2 \text{ and } n_3 \geq 2 \end{cases}.$$

Since $p_2 \geq 3$ and $p_3 \geq 5$, it follows that $\theta > 0$ in all the four cases. This gives $|E_{m_2}| + |E_{m_3}| > |\Gamma|$, a contradiction. \square

Proposition 5.3. *E_{m_2} is disjoint from X .*

Proof. Otherwise, E_{m_2} is contained in Γ by Lemma 2.3. Then, by Proposition 5.2, E_{m_3} is disjoint from X and so is contained either in A or in B .

Case 1: $E_{m_3} \subseteq B$. Since $E_{m_1} \subseteq A$, the subgroup $S_{m_1,3}$ must be contained in Γ and so $|E_{m_2}| + |S_{m_1,3}| \leq |\Gamma|$. We calculate $|E_{m_2}| + |S_{m_1,3}| - |\Gamma|$ using (9). If $n_2 = 1$, then

$$|E_{m_2}| + |S_{m_1,3}| - |\Gamma| \geq 2^{n_1-1} [p_3^{n_3} - 2] > 0.$$

If $n_2 \geq 2$, then

$$\frac{|E_{m_2}| + |S_{m_1,3}| - |\Gamma|}{2^{n_1-1} p_2^{n_2-2}} \geq p_3^{n_3-1} [p_2^2 + \phi(p_2)(p_3 - p_2 - 1)] - 2p_2 > 0.$$

Thus $|E_{m_2}| + |S_{m_1,3}| > |\Gamma|$, a contradiction.

Case 2: $E_{m_3} \subseteq A$. Since $E_{m_2} \subseteq X$ and $A \cup B$ is a separation of $\mathcal{P}(\overline{X})$, the order of any element of B is of the form $2^{n_1} p_2^k p_3^{n_3}$, where $0 \leq k \leq n_2 - 2$ (this is possible only when $n_2 \geq 2$). Let $t \in \{0, 1, \dots, n_2 - 2\}$ be the largest integer for which B has an element of order $2^{n_1} p_2^t p_3^{n_3}$. Then the sets

$$E_{2^{n_1} p_2^{t+1} p_3^{n_3}}, E_{2^{n_1} p_2^{t+2} p_3^{n_3}}, \dots, E_{2^{n_1} p_2^{n_2-2} p_3^{n_3}}, E_{2^{n_1} p_2^{n_2-1} p_3^{n_3}} = E_{m_2}$$

and the two subgroups

$$S_{2^{n_1} p_2^t p_3^{n_3-1}}, S_{2^{n_1-1} p_2^t p_3^{n_3}}$$

are contained in Γ . Set $P = \bigcup_{k=t+1}^{n_2-1} E_{2^{n_1} p_2^k p_3^{n_3}}$ and $Q = S_{2^{n_1} p_2^t p_3^{n_3-1}} \cup S_{2^{n_1-1} p_2^t p_3^{n_3}}$. Then $|P| + |Q| = |P \cup Q| \leq |\Gamma|$. We have $|Q| = 2^{n_1-1} p_2^t p_3^{n_3-1} (p_3 + 1)$ and

$$|P| = \sum_{k=t+1}^{n_2-1} \phi(2^{n_1} p_2^k p_3^{n_3}) = 2^{n_1-1} p_3^{n_3-1} (p_3 - 1) (p_2^{n_2-1} - p_2^t).$$

So

$$\begin{aligned} |P| + |Q| &= 2^{n_1-1} p_3^{n_3-1} \left[(p_3 - 1) (p_2^{n_2-1} - p_2^t) + p_2^t (p_3 + 1) \right] \\ &= 2^{n_1-1} p_2^{n_2-1} p_3^{n_3-1} (p_3 - 1) + 2^{n_1} p_2^t p_3^{n_3-1}. \end{aligned}$$

Then $|P| + |Q| - |\Gamma| \geq 2^{n_1-1} p_2^{n_2-1} [p_3^{n_3-1} (p_3 - p_2) - 2] + 2^{n_1} p_2^t p_3^{n_3-1} > 0$ for any t . This gives $|P| + |Q| > |\Gamma|$, a contradiction. \square

Proposition 5.4. E_{m_2} is contained in A .

Proof. Proposition 5.3 implies that E_{m_2} is contained either in A or in B . Suppose that $E_{m_2} \subseteq B$. Since $E_{m_1} \subseteq A$, the subgroup $S_{m_{1,2}}$ is contained in Γ . Consider the set E_{m_3} , which would be contained either in A, B or Γ . We show that none of these possibilities occurs. If $E_{m_3} \subseteq \Gamma$, then

$$\frac{|E_{m_3}| + |S_{m_{1,2}}| - |\Gamma|}{2^{n_1-1}p_2^{n_2-1}} \geq \begin{cases} p_3 - 2, & \text{if } n_3 = 1 \\ p_3^{n_3-2}(p_3^2 - p_2 + 1) - 2, & \text{if } n_3 \geq 2 \end{cases}.$$

This gives $|E_{m_3}| + |S_{m_{1,2}}| > |\Gamma|$, a contradiction. If $E_{m_3} \subseteq A$, then the subgroup $S_{m_{2,3}}$ is contained in Γ . Since

$$|S_{m_{1,2}} \cup S_{m_{2,3}}| - |\Gamma| \geq 2^{n_1-1}p_2^{n_2-1} \left[p_3^{n_3-1}(p_3 - p_2 + 2) - 2 \right] > 0,$$

we get $|S_{m_{1,2}} \cup S_{m_{2,3}}| > |\Gamma|$, a contradiction. Finally, assume that $E_{m_3} \subseteq B$. Then the subgroup $S_{m_{1,3}}$ is contained in Γ . In this case, we get

$$|S_{m_{1,2}} \cup S_{m_{1,3}}| - |\Gamma| \geq 2^{n_1-1}p_2^{n_2-1} [p_3^{n_3} - 2] > 0,$$

giving $|S_{m_{1,2}} \cup S_{m_{1,3}}| > |\Gamma|$, a contradiction. \square

Proposition 5.5. The order of any element of B is $2^{n_1}p_2^{n_2}$.

Proof. We have $E_{m_1} \subseteq A$ by our assumption and $E_{m_2} \subseteq A$ by Proposition 5.4. Since $A \cup B$ is a separation of $\mathcal{P}(\overline{X})$, the order of any element of B is of the form $2^{n_1}p_2^{n_2}p_3^k$, where $0 \leq k \leq n_3 - 1$. Let $t \in \{0, 1, \dots, n_3 - 1\}$ be the largest integer for which B has an element of order $2^{n_1}p_2^{n_2}p_3^t$ (and so $E_{2^{n_1}p_2^{n_2}p_3^t} \subseteq B$). Then the sets

$$E_{2^{n_1}p_2^{n_2}p_3^{t+1}}, E_{2^{n_1}p_2^{n_2}p_3^{t+2}}, \dots, E_{2^{n_1}p_2^{n_2}p_3^{n_3-1}}$$

and the two subgroups

$$S_{2^{n_1}p_2^{n_2-1}p_3^t}, S_{2^{n_1-1}p_2^{n_2}p_3^t}$$

are contained in Γ . Set $P_1 = \bigcup_{k=t+1}^{n_3-1} E_{2^{n_1}p_2^{n_2}p_3^k}$ and $Q_1 = S_{2^{n_1}p_2^{n_2-1}p_3^t} \cup S_{2^{n_1-1}p_2^{n_2}p_3^t}$. Then $|P_1| + |Q_1| = |P_1 \cup Q_1| \leq |\Gamma|$. On the other hand, we have

$$|Q_1| = 2^{n_1-1}p_2^{n_2-1}p_3^t(p_2 + 1) \text{ and } |P_1| = 2^{n_1-1}p_2^{n_2-1}(p_2 - 1)(p_3^{n_3-1} - p_3^t).$$

So $|P_1| + |Q_1| = 2^{n_1-1}p_2^{n_2-1}p_3^{n_3-1}(p_2 - 1) + 2^{n_1}p_2^{n_2-1}p_3^t$. Then, using (9), we get

$$|P_1| + |Q_1| - |\Gamma| \geq 2^{n_1}p_2^{n_2-1}(p_3^t - 1).$$

If $t \geq 1$, then it would follow that $|P_1| + |Q_1| > |\Gamma|$ which is not possible. So $t = 0$ and every element in B is of order $2^{n_1}p_2^{n_2}$. \square

Now, Proposition 5.5 together with the facts that E_{m_1}, E_{m_2} are contained in A imply the sets $E_{2^{n_1}p_2^{n_2}p_3^k}$ with $k \in \{1, 2, \dots, n_3 - 1\}$ and the two subgroups $S_{2^{n_1}p_2^{n_2-1}}, S_{2^{n_1-1}p_2^{n_2}}$ are contained in Γ . Also $E_n \subseteq X$. Since $Z(3, 0)$ is precisely the union of these sets, it follows that X contains $Z(3, 0)$. Then, by the minimality of $|X|$, we get $X = Z(3, 0)$ and hence

$$\kappa(\mathcal{P}(C_n)) = |X| = |Z(3, 0)| = \phi(n) + 2^{n_1-1}p_2^{n_2-1} \left(p_3^{n_3-1}\phi(p_2) + 2 \right).$$

This completes the proof of Theorem 1.3.

References

- [1] J. Abawajy, A. Kelarev and M. Chowdhury, Power graphs: a survey, *Electron. J. Graph Theory Appl. (EJGTA)* 1 (2013), no. 2, 125–147.
- [2] P. J. Cameron, The power graph of a finite group, II, *J. Group Theory* 13 (2010), no. 6, 779–783.
- [3] I. Chakrabarty, S. Ghosh and M. K. Sen, Undirected power graphs of semigroups, *Semigroup Forum* 78 (2009), no. 3, 410–426.
- [4] S. Chattopadhyay and P. Panigrahi, Connectivity and planarity of power graphs of finite cyclic, dihedral and dicyclic groups, *Algebra Discrete Math.* 18 (2014), no. 1, 42–49.
- [5] S. Chattopadhyay and P. Panigrahi, On Laplacian spectrum of power graphs of finite cyclic and dihedral groups, *Linear Multilinear Algebra* 63 (2015), no. 7, 1345–1355.
- [6] B. Curtin and G. R. Pourgholi, Edge-maximality of power graphs of finite cyclic groups, *J. Algebraic Combin.* 40 (2014), no. 2, 313–330.
- [7] A. Doostabadi, A. Erfanian and A. Jafarzadeh, Some results on the power graphs of finite groups, *ScienceAsia* 41 (2015), 73–78.
- [8] A. Doostabadi and M. F. D. Ghouchan, On the connectivity of proper power graphs of finite groups, *Comm. Algebra* 43 (2015), no. 10, 4305–4319.
- [9] A. V. Kelarev and S. J. Quinn, A combinatorial property and power graphs of groups, in *Contributions to general algebra*, 12 (Vienna, 1999), 229–235, Heyn, Klagenfurt, 2000.
- [10] A. V. Kelarev, S. J. Quinn and R. Smolíková, Power graphs and semigroups of matrices, *Bull. Austral. Math. Soc.* 63 (2001), no. 2, 341–344.
- [11] A. V. Kelarev and S. J. Quinn, Directed graphs and combinatorial properties of semigroups, *J. Algebra* 251 (2002), no. 1, 16–26.
- [12] M. Mirzargar, A. R. Ashrafi and M. J. Nadjafi-Arani, On the power graph of a finite group, *Filomat* 26 (2012), no. 6, 1201–1208.
- [13] A. R. Moghaddamfar, S. Rahbariyan and W. J. Shi, Certain properties of the power graph associated with a finite group, *J. Algebra Appl.* 13 (2014), no. 7, 1450040, 18 pp.

Address:

School of Mathematical Sciences

National Institute of Science Education and Research, Bhubaneswar (HBNI)

At/Po - Jatni, District - Khurda, Odisha - 752050, India.

E-mails: sriparna@niser.ac.in, klpatra@niser.ac.in, bksahoo@niser.ac.in